HIPAA Awareness Training

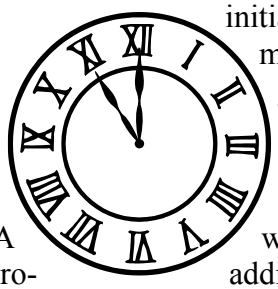
North Dakota Department of Health

Issue 1
March 2003

HIPAA Coordinator & Officers Appointed

Arvy Smith, Deputy State Health Officer, appointed the Health Insurance Accountability and Portability Act (HIPAA) team for the Department of Health. Effective July 1, 2002 Darleen Bartz has taken on the responsibilities of the Department of Health HIPAA Coordinator and Privacy Officer; Bridget Weidner is Assistant Privacy Officer; and Darin Meschke is Security and Transactions Sets Officer.

The team has made much progress since taking on their roles just a few months ago. They have written the NDDoH's HIPAA Privacy Project Plan. They also have been establishing committees, developing HIPAA policies, procedures and forms and have been working with the local public health units to determine their HIPAA level of readiness.



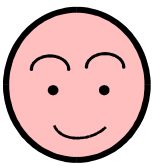
Timing has been crucial in meeting the HIPAA deadlines. Darleen, Bridget and Darin have spent many hours researching and writing in an effort to keep NDDoH HIPAA compliant. The Department has initiated a department-wide program to bring all its impacted entities into compliance with HIPAA. In addition, the NDDoH will be acting as an information resource to the local public health units throughout the state.

You will learn more about HIPAA and how it affects you as a Department of Health employee in the training and resources being provided to you.

Inside this issue:

HIPAA Humor

HIPAA-Ectomy - the removal of individual identifiable health information from records.
HIPAA-Glycemia - the low level of understanding of HIPAA regulations.
HIPAA-Phobia - morbid fear of HIPAA regulations.
HIPAA-Thermia - the unexplained chill that is running down the back of anyone associated with HIPAA.



HIPAA 101

The federal law known as "HIPAA" stands for the Health Insurance Portability and Accountability Act of 1996. This law was passed to promote more standardization and efficiency in the health care industry.

There are four parts to HIPAA's Administrative Simplification:
1. Electronic Transactions and Code Sets Standards requirements
2. Privacy requirements
3. Security requirements
4. National Identifier requirements

HIPAA will directly impact health care providers who transmit any health care information in electronic form in connection with a covered transaction, as well as indirectly impacting their business partners. But these impacts will eventually result in overall improvements in many areas of the health care industry.

The final HIPAA rule for Standards for Privacy of Individually Identifiable Health Information was published on Dec. 28, 2000 in the Federal Register and updated with the final rule modification Aug. 14, 2002. The majority of covered entities that are affected must comply by April 14, 2003. The final rule for Standards for Security was published Feb. 20, 2003 with an effective date of April 21, 2005. The final rule for Transactions and Codes Sets was published on Aug. 17, 2000 in the Federal Register with an effective date of Oct. 16, 2002. An additional year was granted if an extension was filed prior to that date, making the new effective date Oct. 16, 2003.

What is HIPAA Administrative Simplification?

The requirements for each area of HIPAA Administrative Simplification are:

1. Electronic Transactions and Code Sets Standards Requirements
National standards (for formats and data content) are the foundation of this requirement. HIPAA requires every provider who does business electronically to use the same health care transactions, code sets and identifiers. Many of the electronic changes required under HIPAA are highly technical. But, it is important for you to know about the HIPAA Administrative Simplification requirements and how they will impact our Department. Transactions and code sets standards requirements were created to give the health care industry a common language to make it easier to transmit information electronically. The electronic transactions that are directly covered under HIPAA are transmitted by the Division of Microbiology.

2. Privacy Requirements
The privacy requirements limit the release of patient protected health information without the patient's knowledge and consent beyond that required for patient care. Patient's personal information must be more securely guarded and more carefully handled when conducting the business of health care.

3. Security Requirements
The security regulation outlines the minimum administrative, technical and physical safeguards required to prevent unauthorized access to protected health care information. The Department of Health and Human Services published the final HIPAA security rule on Feb. 20, 2003. The general requirements of the security rule include:

- Ensuring confidentiality, integrity and availability of electronic protected health information that a covered entity creates, receives, maintains or transmits;
- Protecting against reasonably anticipated threats or hazards to the security or integrity of information;
- Protecting against reasonably anticipated uses and disclosures not permitted by privacy rules;
- Ensuring compliance by the workforce.

The security rule is expected to aid in the implementation of Department-wide "best practices" for security policies and procedures.

4. National Identifier Requirements
HIPAA will require that health care providers, health plans and employers have standard national numbers that identify them on standard transactions.

The Employer Identification Number, issued by the IRS, was selected as the identifier for employers and was adopted effective July 30, 2002. The remaining identifiers are expected to be determined in the coming year.

What does this regulation do?

The Privacy Rule became effective on April 14, 2001. Most health plans and health care providers that are covered by the new rule must comply with the new requirements by April 2003.

The Privacy Rule for the first time creates national standards to protect individuals' medical records and other personal health information.

- It gives patients more control over their health information.
- It sets boundaries on the use and release of health records.
- It establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information.
- It holds violators accountable, with civil and criminal penalties that can be imposed if they violate patients' privacy rights.
- It strikes a balance when public responsibility requires disclosure of some forms of data - for example, to protect public health.

For patients - it means being able to make informed choices when seeking care and reimbursement for care based on how personal health information may be used.

- It enables patients to find out how their information may be used and what disclosures of their information have been made.

The Privacy Rule must be complied with by April 2003

The Security Rule must be complied with by April 2005

- It generally limits release of information to the minimum reasonably needed for the purpose of the disclosure.
- It gives patients the right to examine and obtain a copy of their own health records and request corrections.

Why is this regulation needed?

In enacting the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Congress mandated the establishment of standards for the privacy of individually identifiable health information.

When it comes to personal information that moves across hospitals, doctors' offices, insurers or third party payers and state lines, our country has relied on a patchwork of federal and state laws. Under the current patchwork of laws, personal health information can be distributed - without either notice or consent - for reasons that have nothing to do with a patient's medical treatment or health care reimbursement. Patient information held by a health plan may be passed on to a lender who may then deny the patient's application for a home mortgage or a credit card - or to an employer who may use it in personnel decisions.

The Privacy Rule establishes a federal floor of safeguards to protect the confidentiality of medical information. State laws which provide stronger privacy protections will continue to apply over and above the new federal privacy standards.

Health care providers have a strong tradition of safeguarding private health information. But in today's world, the old system of paper records in locked filing cabinets is not enough. With information broadly held and transmitted electronically, the rule provides clear standards for all parties regarding protection of personal health information.

(continued from previous page)

What does this regulation require the average provider to do?

For the average health care provider, the Privacy Rule requires activities, such as:

- Providing information to patients about their privacy rights and how their information can be used.
- Adopting clear privacy procedures for its practice, hospital or plan.
- Designating an individual (a Chief Privacy Officer) to be responsible for seeing that the privacy procedures are adopted and followed.
- Securing patient records containing individually identifiable health information so that they are not readily available to those who do not need them.

Responsible health care providers and businesses already take many of the kinds of steps required by the rule to protect patients' privacy. Covered entities of all types and sizes are required to comply with the final Privacy Rule.

To ease the burden of complying with the new requirements, the Privacy Rule gives needed flexibility for providers and plans to create their own privacy procedures, tailored to fit their size and needs.

Who is Impacted by HIPAA?

The HIPAA law applies directly to three specific groups commonly referred to as "covered entities". The three groups include:

1. Health Care Providers who transmit any health information in electronic form in connection with a transaction for which standards requirements have been adopted (i.e. Division of Microbiology.)
2. Health Plans
3. Health Care Clearinghouses

HIPAA, however, indirectly impacts many others in the health care field. For instance, software billing vendors and third party billing services that are not clearinghouses are not required to comply with the law; however, they may need to make changes in order to be able to continue to do business with someone who is "covered" by HIPAA.

The NDDoH has been designated as a hybrid entity. What does this mean and how did we get there?

The NDDoH completed the HIPAA Coverage Determination Report several months ago. This report assisted in determining that the NDDoH was a covered entity. It also allowed the HIPAA team to separate the NDDoH covered functions from those which were not covered functions.

Based on this, it was decided the NDDoH would be classified as a hybrid entity. A hybrid entity is a single legal covered entity whose business activities include both covered and non-covered functions. The NDDoH's covered functions are performed by the Division of Microbiology.

What is protected health information?

Protected health information, commonly referred to as PHI, is health information created or received by a covered entity, that contains patient identification such as name, address, social security number, phone number, zip code, etc. PHI includes all health and individual information whether it is stored on paper, in a computer, on a handheld device or discussed orally.

PHI exists in many places. It may be found:

- In medical and billing records
- In e-mails
- At the fax machine
- On your computers
- In your files
- On your desk
- In telephone conversations or overheard conversations

Look around, you may be surprised at all of the places PHI exists in our environment.

NDDoH Policies and Procedures

The NDDoH HIPAA team has been busy writing HIPAA privacy policies and procedures to bring the NDDoH one step closer to HIPAA compliance. After the policies and procedures were drafted, the HIPAA team met to discuss and revise them further. Then the policies and procedures were brought before the HIPAA privacy workgroup. The HIPAA privacy workgroup consists of Bridget Weidner, Darleen Bartz, Darin Meschke, Deb Arnold, Carmell Barth, Eric Hieb, Danielle Kenneweg, Kirby Kruger and Kerry Olson.

During the HIPAA privacy workgroup meetings, the policies and procedures were discussed based on division concerns. Once the modifications suggested by the HIPAA privacy workgroup were made, the policies and procedures were forwarded to Mike Mullen, Assistant Attorney General, for a legal review. After the legal review is complete and any modifications have been made, all of the policies and procedures will have a final review and approval by Dr. Dwelle and Arvy Smith. The final step is to train NDDoH staff on the policies and procedures. Currently, 27 HIPAA privacy polices and procedures have been developed.

The HIPAA security polices and procedures will go through a similar process prior to implementation.

"When all is said and done, will our healthcare records be used to heal us or reveal us?"

-Donna Shalala, former secretary of Health and Human Services

Uses and Disclosures for Research Activities

The NDDoH may use or disclose protected health information for research purposes if the individual gives a specific written authorization; if the information is de-identified or is part of a limited data set; or without the individual's authorization if there is documentation that a waiver of the individual's authorization has been approved by either an Institutional Review Board or the NDDoH Privacy Board.

The NDDoH is in the process of establishing an Institutional Review Board for the purpose of review and approval of research projects. Arvy Smith, Deputy State Health Officer, has been identified as the chair of this board. Additional members for this board are in the process of being selected and training is planned in the upcoming months for board members. One research project has already been identified which will require review by this board.

The NDDoH Privacy Board will be established this spring within the department. The Privacy Board will be comprised of NDDoH staff with varying backgrounds and appropriate professional competency as necessary to review the request and to ensure that individual privacy rights and interests are maintained. This board must have one member not affiliated with the NDDoH. The Privacy Board will be utilized to review requests for releases of protected health information that do not require IRB approval and monitoring or have been reviewed and approved by an IRB located outside the NDDoH.

HIPAA Complaint Process

Under the HIPAA requirements, an individual who believes a covered entity has violated their privacy has a right to file a complaint with the covered entity and/or the Secretary of the Department of Health and Human Services (DHHS).

If an individual believes the NDDoH has violated their privacy, they must submit their complaint in writing to Privacy Officer, NDDoH, 600 E. Boulevard Ave., Dept. 301, Bismarck ND 58505-0200. Complaints to DHHS need to be sent to U.S. Department of Health and Human Services, 200 Independence Ave S.W., Washington D.C 20201.

ND Department of Health

ND Department of Health
HIPAA Team
600 E Boulevard Ave. Dept. 301
Bismarck, ND 58505-0200

Darleen Bartz, HIPAA Coordinator
Privacy Officer (328.2352)
Bridget Weidner, Assistant Privacy Officer (328.2352)
Darin Meschke, Security and Transactions Officer (328.2494)

We're on the web at www.health.state.nd.us/ndhd/admin/hipaa

HIPAA Links

Centers for Medicare and Medicaid Services (CMS)
HIPAA Gives
HIPAA Help Now
HIPAA Advisory
SNIP WEDI
U.S. Department of Health and Human Services